Commonwealth of Kentucky
Cabinet for Health and Family Services

Information Technology (IT) Policies

KENTUCKY CABINET
FOR HEALTH AND FAMILY SERVICES

010.102 Data/Media Security

Version 2.0
October 14, 2015

Revision History

Date	Version	Description	Author
11/16/2006	1.0	Effective Date	CHFS IT Policies Team Charter
10/14/2015	2.0	Revision Date	CHFS IT Policies Team Charter
10/14/2015	2.0	Review Date	CHFS IT Policies Team Charter

Table of Contents

010.102 Data/Media Security

Category: 010.000 Logical Security

1.1 Policy

All data and media must be sufficiently protected and monitored, consistent with CHFS IT security policies and procedures, to prevent unauthorized use, modification, disclosure, destruction, and denial of service. Security controls must be applied in a manner that is consistent with the value and classification of the data. Access to data must be granted to users only on a "need-to-know" basis, subject to approval by the designated data owner of the information assets. This policy also aligns with all Commonwealth Office of Technology (COT) Enterprise Policies that pertain to Data/Media Security.

1.2 Scope

This policy applies to all CHFS employees and contractors, including all persons providing contractor services, who use, process, or store computerized data relevant to agency business on a CHFS maintained server.

1.3 Policy/Procedure Maintenance Responsibility

The Office of Administrative and Technology Services (OATS) IT Security & Audit Section is responsible for the maintenance of this policy.

1.4 Applicability

All CHFS employees and contractors shall adhere to the following policies.

1.5 Exceptions

Any exceptions to this policy must follow the procedures established in CHFS IT Policy #070.203.

1.6 Data Classification

All CHFS data must be appropriately reviewed by the owner of the data and reviewed by the IT Security & Audit Section to determine its level of sensitivity and/or criticality. If the environment has a mixed set of classified data, the classification that requires the most stringent controls must be used. Any exception to this policy requires approval by the CHFS IT Security & Audit Section.

1.7 External Markings

All media shall contain external restrictive markings where feasible for easy identification as CHFS property and data sensitivity. Media belonging to external vendors that is in the care of CHFS employee/contractors is subject to the same restrictions.

1.8 Printing/Display

The restrictive markings, including destruction and retention instructions, must be affixed to all media output, e.g., hardcopy and video displays, to warn users of the degree of protection needed.

1.9 Reproduction

Whenever sensitive cabinet and/or agency documents/media are reproduced in total or in part, the reproductions shall bear the same restrictive legends as the original. Reproductions of sensitive media shall be kept to the minimum number of copies required. All CHFS employees and contractors are responsible to ensure that any confidential information that is printed to a central printer is picked up immediately.

1.10 Storage

All media entering or leaving offices, processing areas, or storage facilities must be appropriately controlled. Storage areas and facilities for sensitive media shall be secured and all filing cabinets provided with locking devices appropriate to their sensitivity and protective requirements.

1.11 Disposal/Destruction

All sensitive information shall be afforded special handling regarding its disposal/destruction. This may include the use of shredders, special burn facilities, or other measures approved by the CHFS IT Security & Audit Section.

1.12 Shipping and Manual Handling

CHFS data must not be supplied to vendors, contractors or other external organizations without properly executed contracts and confidentiality agreements specifying conditions of use, security requirements, and return dates. When shipping sensitive information, verify receipt of delivery. (Except where required by law or statutory regulation)

1.13 Facsimile Transmission

If sensitive information is to be sent by fax, the recipient must first have been notified of the time when it will be transmitted, and also have agreed that an authorized person will be present at the destination machine when the material is sent. An exception will be made if the area surrounding the fax machine is physically restricted such that persons who are not authorized to see the material being faxed may not enter. Individuals may also use CHFS fax service where faxes are directed to their inbox, thus providing a higher degree of security.

When sensitive data must be faxed, a CHFS transmittal cover sheet must first be sent and acknowledged by the recipient. After this is performed, the data may be sent via another call occurring immediately thereafter.

Sensitive CHFS data must not be faxed via non-trusted intermediaries like hotel staff, rented mailbox store staff, etc.

1.14 Electronic Transmission (E-mail, File Transfer Protocol, etc.)

If sensitive data is sent via the Internet or other unsecured media transmission facility, the data must be sent encrypted. Current encryption solutions include Virtual Private Networking (VPN) on the Kentucky Information Highway (KIH), Secure Hypertext Transfer Protocol (HTTPS), Secure Socket Layer (SSL), secure FTP, Secure Shell (SSH), and Entrust Express for encrypting e-mails.

1.15 Electronic Media

Sensitive or Confidential data stored on removable devices including, but not limited to CD’s, Thumb Drives, External Drives or stored on portable workstations or mobile devices including, but not limited to laptops or handheld devices, must be protected by data encryption and the appropriate password protection (see CHFS IT Policy #020.307 & CHFS IT Policy #020.309).

When possible, all sensitive data should be stored on CHFS protected servers. Only sub sets of data should be downloaded to a workstation/portable device to perform a work related function.

Laptops and mobile devices should be configured by CHFS IT personnel to ensure the maximum level of security necessary to protect any sensitive data downloaded to that device.

At no time shall personal removable storage devices (devices not issued by CHFS IT) be attached to state owned workstations for the purpose of storing and/or retrieving electronic data (see CHFS IT Policy #070.102.).

1.16 Review Cycle

Annual

1.17 Cross Reference(s)

- CHFS IT Policy #070.102 – Personal Hardware/Software
- CHFS IT Policy # 070.203 – Exceptions to Standards and Policies
- KRS 434.855 - Misuse of computer information
- KRS 514.030 - Theft by unlawful taking or disposition